Section III: **Application Security**
Title: **Web Security Standard**
Current Effective Date: **June 30, 2008**
Revision History: **June 5, 2008**
Original Effective Date: **June 30, 2008**

Purpose: To protect North Carolina (NC) Department of Health and Human Services (DHHS) information resources that are exposed to additional security threats when used for information sharing over the World Wide Web (WWW).

STANDARD

1.0 Background

In the process of business automation, web application architecture has been widely chosen as the architecture of choice. Such architecture can be harnessed to enable near universal access to an organization's information resources. Without proper safeguards, that architecture can also be subverted in ways that cause harm to the organization or the individuals about whom the information resources pertain. This standard will address strategies and guidelines to provide assurances that the information resources are being used by only those that are intended by the organization and that the integrity of the resources is being preserved.

2.0 Developing a Web Site

Development of Web sites shall incorporate secure development best practices. Industry standards for securing operating systems and Web server software include, but are not limited to, the National Security Agency (NSA) and SANS Institute guidelines. These standards should be used for guidance in securely configuring and hardening Web sites.

Development Web sites shall be isolated from production and user desktop networks to prevent remote compromise while the server is being built and the web application developed. Development servers/applications shall be developed and tested with input validation to protect against data validation weaknesses in the Web application's design. Network and application (Web/database) vulnerability scans should be run against development servers during and after the development process to ensure that a server/Web application is built securely.

3.0 Maintaining a Web Site

Divisions and Offices shall ensure that:

- Web sites are kept up to date and secure and that the information they present is accurate
- Web sites are hardened and that standard security configurations based on industry guidelines and standards are adhered to

- Secure authentication is used to protect the security of Web servers that have access to confidential information or applications that perform critical functions
- Secure authentication must be performed under Secure Socket Layer (SSL) transfer only
- SSL certificates shall remain active and be issued only from a valid certificate authority. Self-signed SSL certificates shall be limited to only test environments. Expired certificates shall be replaced with a valid active certificate
- Web sites have the latest operating system and application patches
- Web site logs are periodically reviewed
- The number of personnel with administrative access is limited to only qualified and appropriate individuals
- Web sites are available to the appropriate users (public and private)
- Unauthorized modification of the Web site's information is quickly discovered and resolved
- All sites that the Divisions and Offices are responsible for are periodically tested for vulnerabilities
- All sites comply with federal and state laws and regulations as well as State, Department, and Division policies and standards
- Network and application (Web/database) vulnerability scans should be regularly run against all production Web servers to ensure a secure posture

Any passwords used by a server, Web server, Web application, or any other related applications need to meet complexity levels and have change cycles appropriate to the level of risk posed by potential compromise of the system. Credentials must only pass over SSL connections. Completed Web sites should be periodically searched with a Web search engine by development staff to ensure that there is no access to Web information beyond what is intended.

In addition, the following should be considered:

- The use of file integrity checking software to detect the modification of static or critical files on the server is strongly recommended
- Web applications should be developed to use a minimum number of ports to allow for easy integration in traditional demilitarized zone (DMZ—filtered subnet) environments

See the NC Statewide Information Security Manual, Version No. 1 - Chapter 03 – Processing Information and Documents, Standard: 030309: Developing a Web Site for more guidelines and information.

Reference:

- NC Statewide Information Security Manual, Version No. 1
  - Chapter 03 – Processing Information and Documents, Section 03: Email and the World Wide Web
    - Standard 030309 - Developing a Web Site
    - Standard 030316 - Maintaining Your Web Site